



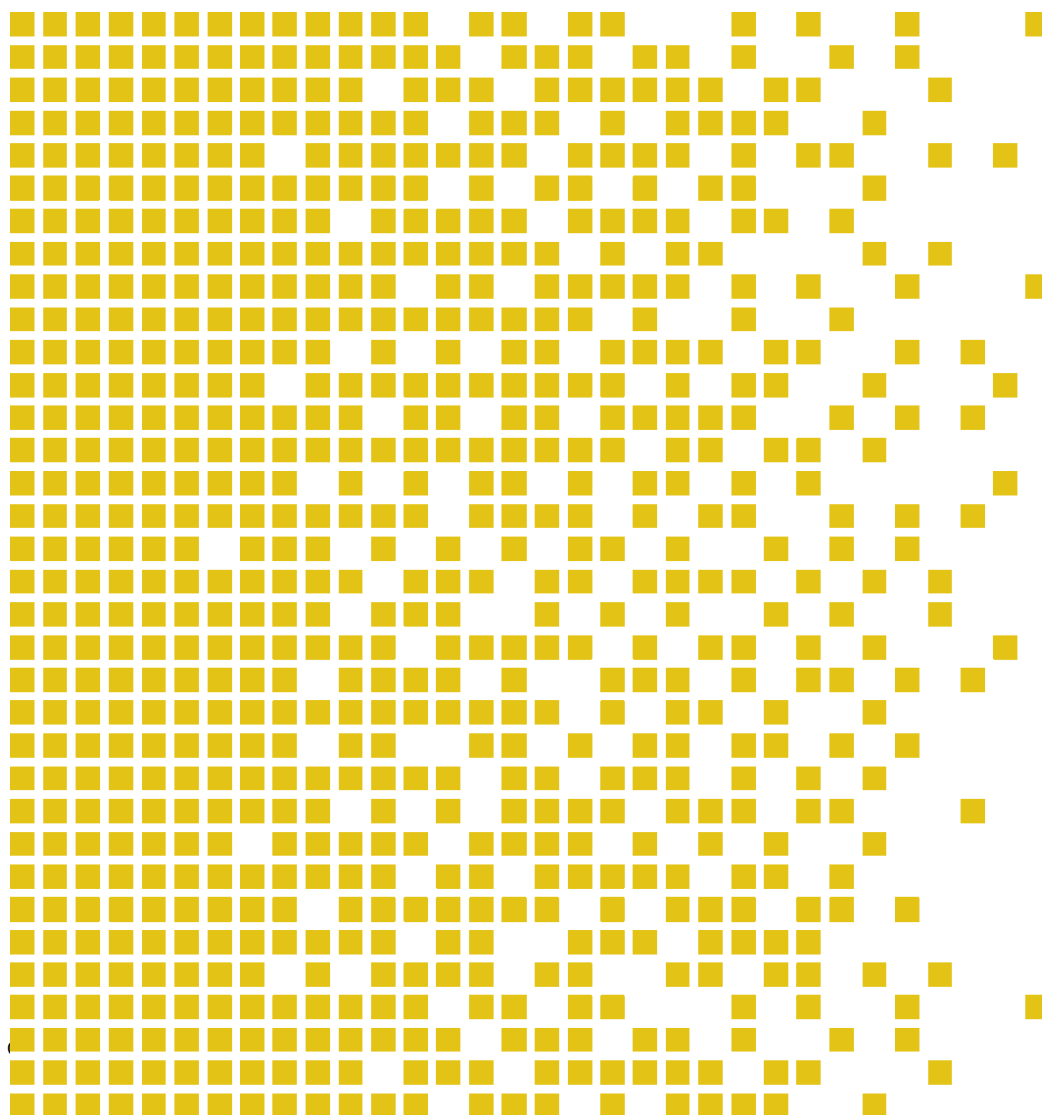
SERTIT-060 CR Certification Report

Issue 1.0 01 February 2016

TSF 201

HW version: 3AQ 25960 BAAA rev. C.

SW version: 3AQ 25950 AAAA rev. 2.2 build 0013.



**ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN
THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of the CCRA May 23rd 2000. The recognition under CCRA is limited EAL 4 and ALC_FLR CC part 3 components.



**MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY
EVALUATION CERTIFICATES (SOGIS MRA)**

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual Recognition under the SOGIS MRA recognition agreement applies to EAL 4.





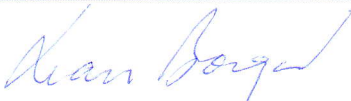
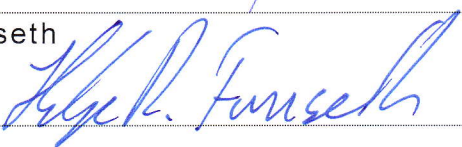
Contents

1	Certification Statement	4
2	Abbreviations	5
3	References	6
4	Executive Summary	7
4.1	Introduction	7
4.2	Evaluated Product	7
4.3	TOE scope	7
4.4	Protection Profile Conformance	7
4.5	Assurance Level	7
4.6	Security Policy	7
4.7	Security Claims	8
4.8	Threats Countered by the TOE and TOE environment.	8
4.9	Threats and Attacks not Countered	8
4.10	Environmental Assumptions and Dependencies	8
4.11	IT Security Objectives	9
4.12	Non-IT Security Objectives	10
4.13	Security Functional components	11
4.14	Security Function Policy	11
4.15	Evaluation Conduct	12
4.16	General Points	12
5	Evaluation Findings	14
5.1	Introduction	14
5.2	Delivery	14
5.3	Installation and Guidance Documentation	14
5.4	Misuse	14
5.5	Vulnerability Analysis	14
5.6	Developer's Tests	14
5.7	Evaluators' Tests	15
6	Evaluation Outcome	16
6.1	Certification Result	16
6.2	Recommendations	16
	Annex A: Evaluated Configuration	17
	TOE Identification	17
	TOE Documentation	17
	TOE Configuration	17

1 Certification Statement

Thales Norway AS Trusted Security Filter TSF 201 is a contents-filtering gateway consisting of both hardware and software. It enables data transfer in a secure manner between two IP networks of different security classifications.

Trusted Security Filter TSF 201 HW version: 3AQ 25960 BAAA rev. C. SW version: 3AQ 25950 AAAA rev. 2.2 build 0013. has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant components of Evaluation Assurance Level EAL5 augmented with ALC_FLR.3 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality when running on the platforms specified in Annex A.

Author	Rage, Arne Høye Certifier 
Quality Assurance	Lars Borgos Quality Assurance 
Approved	Helge Rager Furuseth Head of SERTIT 
Date approved	01 February 2016

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCI	Controlled Cryptographic Item
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
FPGA	Field-programmable gate array
ISO/IEC 15408	Information technology -- Security techniques -- Evaluation criteria for IT security
NSM	Norwegian National Security Authority
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Function Interface
TSP	TOE Security Policy



3 References

- [1] Trusted Security Filter TSF 201, Security Target 3AQ 25940 AAAA Revision 2, 14 September 2015
- [2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2012-09-001, Version 3.1 R4, September 2012.
- [3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CCMB-2012-09-002, Version 3.1 R4, September 2012.
- [4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2012-09-003, Version 3.1 R4, September 2012.
- [5] The Norwegian Certification Scheme, SD001E, Version 9.0, 02 April 2013.
- [6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.
- [7] Common Criteria EAL5 Evaluation of Trusted Security Filter (TSF 201) Evaluation Technical Report v 1.1, 29.01.2016.
- [8] SOGIS MRA, Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Version 3.0, January 8th 2010.
- [9] Forskrift om informasjonssikkerhet FOR-2001-07-01-744

Supporting guidance documents are listed in Annex A.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Trusted Security Filter TSF 201 version HW version: 3AQ 25960 BAAA rev. C. SW version: 3AQ 25950 AAAA rev. 2.2 build 0013. to the Developer, Thales Norway AS, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation components.

4.2 Evaluated Product

The product evaluated was Trusted Security Filter TSF 201 with HW version: 3AQ 25960 BAAA rev. C. SW version: 3AQ 25950 AAAA rev. 2.2 build 0013.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Thales Norway AS

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

Trusted Security Filter (TSF 201) with

HW version: 3AQ 25960 BAAA rev. C

SW version: 3AQ 25950 BAAA rev. 2.2 build 013

The TEMPEST certification is not within the scope of this CC evaluation.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target[1] specified the assurance components for the evaluation. Predefined evaluation assurance level EAL5 augmented with ALC_FLR.3 was used. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

Cryptographic key destruction method meets NSM guidelines.

There are no Organizational Security Policies or rules with which the TOE must comply.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional components and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered by the TOE and the TOE environment.

- T.CONN.HIGH.LOW - Information with HIGH security classification on the HIGH network may be transferred to the LOW network.
- T.TAMPERING - Security-critical part of the TOE may be subject to physical attack that may compromise security.
- T.MISUSE - An attacker may transfer information classified HIGH from the HIGH network to the LOW network, by the use of data messages.
- T.TEMPEST - Electromagnetic emanations may divulge classified information.
- T.UNAUTHORISED.USE - Authorised persons on the HIGH system may perform unauthorised use of the HIGH system's applications and management system.
- T.ILLEGAL.CONFIG - An attacker attempts to: Modify or destroy authorised filter configuration files, modify or destroy keys used for decryption of filter configuration files, inject unauthorised filter configuration files or inject malicious code into the TOE by unauthorised access through the administration interface.
- T.SECURE.KEY - An attacker attempts to obtain the cryptographic keys for the purpose of decrypting and modifying the filter configuration files.

4.9 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.10 Environmental Assumptions and Dependencies

- A.PHYSICAL - The system comprising the TOE and the HIGH network is installed in a physical protected area, minimum approved for information classified HIGH. This applies also to the local management and the channel from the local management. The LOW network is installed in a physical area minimum approved for protection of the information classified LOW.
- A.TRAINING - All TOE managers are trained in the correct use of the TOE.



- A.CLEARANCE - All TOE managers have a minimum clearance for the security level HIGH, and is authorised for all information handled by the system.
- A.MAN.AUTHORISED - Only managers with special authorisation are allowed to do configuration and management of the system including TOE.
- A.USAGE - The TOE is used between two LANs in a protected environment and is installed according to the installation guidelines for the TOE.

4.11 IT Security Objectives

- O.ALARM.FAILURE - If a hardware or software failure is detected in the TOE, the TOE shall raise a local alarm.
- O.AUDIT - The TOE shall have a protected audit log (residing in permanent memory and not possible to delete by the user) that can be viewed by a web browser on the HIGH network.
- O.CRYPTO - The TOE shall have cryptographic functions to decrypt filter configuration files and software update files for encryption of internal keys.
- O.FW.THRESHOLD - The TOE shall count rejected messages and perform flow monitoring of messages handled by the filter and shall generate an audit event if the threshold of legitimate messages is exceeded.
- O.FILTER - Information classified HIGH shall be prevented from being transmitted to the LOW network.
- O.KEY.GENERATE - The TOE shall have a mechanism to generate cryptographic keys that are for internal use only.
- O.KEY.LOAD - The TOE shall have a mechanism to load cryptographic keys. The keys shall be integrity protected.
- O.NO.CONFIG - The firewall filter shall not be configurable inside the TOE. The TOE manager shall be able to select sets of predefined filter criteria.
- O.ROBUST.TOE.ACCESS - The TOE shall provide mechanisms that control the administrator's logical access to the TOE local management interface and to explicitly deny access to non-authorised users. The TOE shall provide two operator roles (users): Operator and Security operator (access to both operator and security operator functions). Authentication of users shall be based on pin code (optional), operator role and password.
- O.SECURE.CHANNEL - The TOE shall use asymmetric encryption techniques to establish a secure channel between the TOE and a web client presenting the local management information.
- O.SECURE.CONFIGURATION - TOE filter files and software update files can be loaded from the local management interface. Filter configuration files and software are protected by encryption and digital signature. Prior to accepting a new file, the TOE shall perform the

following verification: The file shall be decrypted, the integrity and authenticity shall be verified by means of a digital signature, Known Answer Tests shall be run (filters only). If the decryption and verification of signature fails or Known Answer Test fails, the update shall be rejected.

- O.SELF.TEST - Security critical functions shall be tested by a combination of power-up tests, periodic tests and continuous tests.
- O.EMERGENCY.ERASE - The TOE shall provide automatic and manual functions for emergency erase of cryptographic keys and filter configuration files. The emergency erase shall be triggered automatically upon tamper detection or be manually initiated from the front panel.
- OE.AUDIT - The IT environment shall be able to display the web page with the audit log. The web server resides in the TOE and the audit log is protected by the TOE
- OE.KEY.GENERATE - The IT environment shall be able to generate cryptographic keys that the TOE uses to decrypt filter configuration files and software update files. The cryptographic keys shall be administered according to Forskrift om informasjonsikkerhet[9] – kapittel 7 Administrativ kryptosikkerhet.
- OE.MAN.ACCESS - Special authorisation is required to grant access to configure and manage the TOE.

4.12 Non-IT Security Objectives

- NO.SEALING - The TOE shall be sealed in such a way that it is easy to see that it has been opened/tampered with.
- NO.TEMPEST - TEMPEST evaluation and certification of the TOE is performed by NSM. This certification ensures that NO.TEMPEST is achieved.
- NOE.ACCESS.CTRL - Only authorised persons shall be given physical access to the system comprising the TOE and the HIGH network.
- NOE.AUDIT - Authorised managers of the TOE must ensure that the TOE audit log are used and managed effectively. On particular, TOE audit log should be inspected on a regular basis, appropriate and timely action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future.
- NOE.CI - The TOE shall be treated as CCI material according to Forskrift om informasjonsikkerhet [9] – kapittel 7 Administrativ kryptosikkerhet.
- NOE.CLEARANCE - All users shall have a minimum clearance for the maximum-security level of information handled in the system.
- NOE.INSTALL - The responsible for the TOE must ensure that the TOE is installed according to the installation guidelines for the TOE.
- NOE.KEY.DESTRUCT - The cryptographic keys shall be destructed according to Forskrift om informasjonsikkerhet[9] – kapittel 7 Administrativ kryptosikkerhet.



- NOE.MAN.TRAIN - The TOE managers are fully trained to use and interpret the TOE equipment.
- NOE.PHYS.PROT - The site where the TOE is installed shall have physical protection. The level of protection shall be approved for minimum security level HIGH.

4.13 Security Functional components

- FAU_ARP.1 Security alarms
- FAU_GEN.1 Audit data generation
- FAU_SAA.1 Potential violation analysis
- FAU_SAR.1 Security audit review
- FAU_STG.1 Protected audit trail storage
- FCS_COP.1(1) Cryptographic operation (filter configuration and SW update files)
- FCS_COP.1(2) Cryptographic operation (local management communication)
- FCS_CKM.1 Cryptographic key generation
- FCS_CKM.4 Cryptographic key destruction
- FDP_ACC.1 Subset access control
- FDP_ACF.1 Access control functions
- FDP_IFC.2 Complete information flow control
- FDP_IFF.1 Simple security attributes
- FDP_IFF.6 Illicit information flow monitoring
- FDP_ITC.2 Import from outside of the TOE
- FIA_ATD.1 User attribute definition
- FIA_UAU.1 User authentication
- FIA_UID.2 User identification
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialization
- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles
- FPT_FLS.1 Failure with preservation of secure state
- FPT_PHP.1 Passive detection of physical attack
- FPT_STM.1 Reliable Time Stamps
- FPT_TDC.1 Inter-TSF basic TSF data consistency
- FPT_TST.1 TSF self test
- FTP_ITC.1 Inter-TSF trusted channel

4.14 Security Function Policy

- Traffic_Data Information Flow Control Policy: The Traffic_Data information flow control policy regulates how the TOE shall maintain the network separation security policy. The SFP is defined by FDP_IFC.2 and FDP_IFF.1 The Traffic_Data information flow control policy is monitored for illicit information defined by FDP_IFF.6.

- Configuration Access Control Policy: The Configuration access control policy regulates the access to Security Configuration including authentication of the role Security operator at login. The SFP as defined by FDP_ACC.1 and FDP_ACF.1. The Configuration access control policy is referenced in FDP_ITC.2, ensuring a secure import of filter configuration files and software update files, and also ensuring a secure loading of cryptographic keys through a dedicated interface and trusted channel FDP_ITC.1.

4.15 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by NTT Com Security (Norway) AS Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR)[7] to SERTIT in 29 January 2016. SERTIT then produced this Certification Report.

4.16 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any



other organization that recognizes or gives effect to this Certification Report is either expressed or implied.



5 Evaluation Findings

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

The installation and guidance documents are listed in annex A.

5.4 Misuse

Administrators should follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner. The guidance documents adequately describe all possible modes of operation of the TOE, all assumptions about the intended environment and all requirements for external security.

5.5 Vulnerability Analysis

The evaluators were satisfied that the developer's vulnerability analysis describes all obvious vulnerabilities and that it gives a rationale for why they are / are not exploitable in the intended environment for the TOE.

The evaluators' vulnerability analysis was based on the visibility of the TOE given by the evaluation process.

The evaluators produced and conducted penetration tests on the basis of the developer's vulnerability analysis and their independent vulnerability analysis

5.6 Developer's Tests

The evaluators have confirmed during the evaluation that the developer has thoroughly tested all TSFIs of the TSF 201. The testing was divided in 4 parts:

- Software Integration tests which are performed on the actual version of both hardware and software.
- Software System tests which are performed on the actual version of both hardware and software.



- FPGA tests are intended for functional top-level simulation of the TSF 201 crypto modules.
- Hardware tests where many of these tests are performed under normal laboratory conditions.

5.7 Evaluators' Tests

The evaluators have devised a subset of the developer's test covering all TSFIs, internal interfaces and modules. This subset is about 39% of the total number of developer's tests.

The evaluators have also devised a number of independent tests covering both external and internal interfaces. The test strategy was based on an assessment of who are the threat agents and the assets protected by the TOE.



6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Trusted Security Filter TSF 201 version HW version: 3AQ 25960 BAAA rev. C. SW version: 3AQ 25950 AAAA rev. 2.2 build 0013. meets the Common Criteria Part 3 augmented components of Evaluation Assurance Level EAL5 augmented with ALC_FLR.3 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of Trusted Security Filter TSF 201 version HW version: 3AQ 25960 BAAA rev. C. SW version: 3AQ 25950 AAAA rev. 2.2 build 0013. should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 4.3 "TOE Scope" and Section 5 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

- HW version: 3AQ 25960 BAAA rev. C.
- SW version: 3AQ 25950 AAAA rev. 2.2 build 0013

TOE Documentation

The supporting guidance documents evaluated were:

- [a] Security Target 3AQ 25940 AAAA 377 Ed1
- [b] Security Architecture (SAD) 3AQ 25940 AAAA 549 Ed4
- [c] Software Design Description (SDD) 3AQ 25950 AAAA 549 Ed6
- [d] Operator Manual 3AQ 41228 ABAA EO Ed2
- [e] Integration, Verification, Validation and Qualification Plan (IVVQP) 3AQ 25940 AAAA 440 Ed1
- [f] System Test Procedure (STP) 3AQ 25940 AAAA 206 Ed7

TOE Configuration

The following configuration was used for testing:

